AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (currently amended) A method ~~Method~~ of making an electronic entity with encrypted access secure when said electronic entity ~~comprises means for~~ executing a cryptographic algorithm consisting in applying to an input message a succession of groups of operations known as "rounds" involving a series of respective sub-keys ~~(K_0 ... K_n)~~ produced successively by an iterative process starting from an initial key K, the ~~which~~ method ~~is characterized in that it consists in~~ comprises performing steps of said iterative process so as to obtain a result of an iterative step,

storing in said electronic entity said ~~a~~ result of said ~~an~~ intermediate step ~~(R_n, K_n) of said iterative process~~,

repeating at least some of the steps of said iterative process until a result is recalculated corresponding to the result that has been stored,

comparing the value of said stored result to the value of the corresponding recalculated result, and

prohibiting the broadcasting of an encrypted message ~~(MC)~~ resulting from the application of said algorithm if said two values are different.

2. (currently amended) The method ~~Method~~ according to claim 1, ~~characterized in that it consists in~~ further comprising:

storing a sub-key ~~(K_n)~~ and repeating at least some of the steps of said iterative process until a sub-key is recalculated corresponding to said stored sub-key.

3. (currently amended) The method ~~Method~~ according to claim 1, ~~characterized in that it consists in~~ further comprising:

storing the value of an intermediate result (R_m) of said iterative process and repeating at least a portion of said iterative process until an intermediate result is recalculated corresponding to the stored intermediate result.

4. (currently amended) The method ~~Method~~ according to claim 2, ~~characterized in that it consists in~~ further comprising:

storing the value of the final sub-key (K_n) and repeating at least a final portion of the steps of producing the succession of said sub-keys until said final sub-key is calculated a second time.

5. (currently amended) The method ~~Method~~ according to claim 4, ~~characterized in that it consists in~~ further comprising:

repeating all of the steps of producing the succession of said sub-keys.

6. (currently amended) The method ~~Method~~ according to claim 1, ~~characterized in that it is~~ wherein the method is applied to an ~~a so-called~~ AES algorithm ~~that is known *per se*~~.

7. (currently amended) The method ~~Method~~ according to claim 1, ~~characterized in that it is~~ wherein the method applied to a ~~so-called~~ DES algorithm ~~that is known *per se*~~.

8. (currently amended) An autonomous ~~Autonomous~~ electronic entity ~~characterized in that~~wherein it comprises means (13) for implementing the method according to claim 1.

9. (currently amended) An electronic ~~Electronic~~ entity according to claim 8, ~~characterized in that~~wherein it takes the form of a microcircuit card.